**MÓDULO INV\_SBOX**

Em um projeto de AES (Advanced Encryption Standard) implementado em Verilog, o módulo inv\_sbox é utilizado exclusivamente na etapa de descriptografia (decifra). Ele corresponde à SubBytes inversa da operação de criptografia.

Na descriptografia AES, cada byte do estado é substituído usando uma caixa S inversa (inversa da S-Box usada na criptografia). Isso é necessário para reverter a operação de substituição feita durante a criptografia.

Ordem geral das etapas de descriptografia AES (modo direto):

1. AddRoundKey
2. InvShiftRows
3. InvSubBytes ⟵ aqui entra a inv\_sbox
4. InvMixColumns (exceto na última rodada)

Conclusão:

* inv\_sbox implementa a substituição inversa de bytes no AES.
* É usada apenas na descriptografia.
* Opera byte a byte (8 bits), revertendo os valores aplicados pela sbox.
* Na versão de 128 bits, o inv\_sbox\_128 aplica a inversão aos 16 bytes do bloco.
* A tabela contém a S-Box inversa oficial do AES, conforme o padrão FIPS-197.